GENERALIZED LAYER-2 VPNs

RELATED U.S. APPLICATION DATA

[0001]   Provisional application No. 60/410,862 filed on September 13, 2002.

FIELD OF THE INVENTION

[0002]   The present invention relates to switched virtual circuit (SVC) Layer-2 and layer-1 virtual private networks (L2VPNs and L1VPNs) and is particularly concerned with generalized L2VPNs using point-to-point connectivity to provide connections across provider networks.

BACKGROUND OF THE INVENTION

[0003]   A Virtual Private Network (VPN) may be thought of as a private network constructed within a shared network infrastructure.   In common terminology, these private networks are used by clients while the network infrastructure is supplied by providers.

[0004]   Existing varieties of switched Layer-2 and/or Layer-1 VPNs have limitations affecting ease of implementation and use including:

[0005]   - clients must store and manipulate provider addresses;

[0006]   - clients need to be configured with all the provider addresses to which the client has a site attached;

[0007]   - clients need to know about connection restrictions, such as for closed-user-group (CUG) values, and need to signal these values when establishing connectivity;

[0008]   - clients encounter complexity in managing CUG rules; and

[0009]   - clients need to implement an appropriate Layer-2 and/or layer-1 signalling mechanism proper to the transport technology.

[0010]   In view of the foregoing, it would be desirable to provide a technique for providing generalized Layer-2 virtual private networks (GL2VPNs) which overcomes the above-described inadequacies and shortcomings.

SUMMARY OF THE INVENTION

[0011]   An object of the present invention is to provide an improved generalized Layer-2 Virtual Private Network.

[0012]   According to an aspect of the present invention there is provided a network for providing generalized Layer-2 VPNs, wherein the network includes a set of elements interconnected by services; at least one first subset of the elements defining a private network; and at least one second subset of elements different from said first subset defining a provider network wherein at least two subgroups of the first subset of elements may be connected via the provider network. The network also includes a provisioning mechanism used to define element membership in said first subset of elements; and a signalling mechanism used to create pseudo-wire connectivity between elements within the first subset of elements and across the second subset of elements at the Layer-2 and/or Layer-1 level.

[0013]   Advantages of the present invention include the capability to support any Layer-2 and/or layer-1 VPN service to any network type using scalable common Layer-2 connections, and virtual private networks. GL2VPN does not restrict the layer-3, 2, and 1 service provider to a particular transport or technology used within the provider network. GL2VPN architecture includes intelligent functions for:

[0014]   – Smart QoS handling;

[0015]   – Generalized Single-sided signalling;

[0016]   – a generalized auto-discovery mechanism;

[0017]   – VPN membership distribution;

[0018]   – VPN network selection; and

[0019] – Inter-network service resiliency.

[0020] Generalized Layer-2 virtual private networks provide this capability using open technology.

[0021]

[0022] Conveniently the invention further provides for a network discovery mechanism used to propagate membership information regarding elements which are members of the first subset; and a service discovery mechanism used to propagate services information regarding services interconnecting elements in the first subset with elements in the second subset.

[0023] Also conveniently, the invention further provides for a manager mechanism having a first portion used to effect connection admission control and a second portion used to select encapsulation in response to a connection request; a multi-service tunnel selector mechanism used to create connectivity across the provider network; and a single-sided signalling mechanism used to initiate said connection request triggered by an element of the first subset.

[0024] In accordance with another aspect of the present invention, there is provided a method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of the elements defines a private network and at least one second subset of elements different from the first subset defines a provider network and wherein at least two subgroups of the first subset of elements may be connected via the provider network. The method includes the steps of defining element membership in the first subset of elements via a provisioning mechanism; and creating pseudo-wire connectivity between elements within said first subset of elements at the Layer-2 and/or Layer-1 level across said second subset of elements via a signalling mechanism.

[0025] Conveniently, the method may further include the steps of propagating membership information regarding elements which are members of said first subset via a network discovery mechanism; and propagating services information regarding services interconnecting elements in said first subset with elements in said second

subset via a service discovery mechanism. Further, the method may also conveniently contain the steps of effecting connection admission control via a first portion of a manager mechanism; selecting an encapsulation protocol in response to a connection request via a second portion of a manager mechanism; creating connectivity across the provider network via a multi-service tunnel selector mechanism; and initiating the connection request in response to a trigger by an element of the first subset via a single-sided signalling mechanism.

[0026]   The present invention will now be described in more detail with reference to exemplary embodiments thereof as shown in the appended drawings. While the present invention is described below with reference to the preferred embodiments, it should be understood that the present invention is not limited thereto. Those of ordinary skill in the art having access to the teachings herein will recognize additional implementations, modifications, and embodiments which are within the scope of the present invention as disclosed and claimed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027]   The invention will be further understood from the following detailed description of embodiments of the invention and accompanying drawings in which:

[0028]   **FIG. 1** is a diagram of a generic network having a shared network infrastructure and Virtual Private Networks associated thereto;

[0029]   **FIG. 2** is a block diagram of generalized Layer-2 VPN mechanisms according to an embodiment of the invention;

[0030]   **FIG. 3** is a diagram showing network-side services in relation to access-side services according to an embodiment of the invention;

[0031]   **FIG. 4** is a diagram showing a Layer-2 connection according to the network-side and access-side services of FIG. 3; and

[0032]   **FIG. 5** is a diagram of the main modules of a generalized L2VPN system according to an embodiment of the invention.

[0033] # DETAILED DESCRIPTION

[0034] **Glossary of Acronyms Used**

P – Provider Device

PE – Provider Edge Device

CE – Customer Edge Device

SVC – Switched Virtual Circuit

PIT – Port Information Table

BGP – Border Gateway Protocol

BGP-AD – BGP Auto-Discovery

MPLS – Multi-Protocol Label Switching

DLCI – Data Link Connection Identifier

LMP – Link Management Protocol

ISP – Internet Service Provider

[0035] Referring to **FIG. 1**, there may be seen a generic network having a shared network infrastructure **100** with connected virtual private network sites **101**. The VPN sites **101** make use of the network infrastructure **100** to interconnect physically remote sub-networks of particular VPNs.

[0036] Several key aspects of the operation of generalized L2VPNs include:

[0037] – the control is decoupled from data plane;

[0038] – the access signalling protocols are decoupled from transport signalling.

[0039] – the transport layer decides whether it can meet the access QoS requirements;

[0040] – support is provided for N:1 type connections;

[0041] – support is provided for ATM, FR, Ethernet, MPLS L2VPNs, SONET/SDH; and

[0042] – additionally there is the potential capability for handling proprietary transport-based mechanisms; and

[0043]   – GL2VPN makes the decision on what network to use should any decision be required.

[0044]   The list of generalized Layer-2 VPN access support includes:

[0045]   •   Frame Relay VPN

[0046]   •   ATM VPN

[0047]   •   Ethernet VPN

[0048]   •   Frame Relay to ATM VPNs

[0049]   •   Frame Relay to Ethernet VPNs

[0050]   •   ATM to Ethernet VPNs

[0051]   •   ATM to MPLS

[0052]   •   Frame Relay to MPLS,

[0053]   •   Ethernet to MPLS

[0054]   •   Any to MPLS/IP to Any access.

[0055]   Functions supported by generalized Layer-2 VPN include:

[0056]   •   Generalized single-sided signalling extensions including:

[0057]   – Interworking with Martini-type protocols and providing flexibility in terms of signalling, endpoint identification, and auto-discovery interaction;

[0058]   – supporting Generalized Pseudo-wire (GPW) that can include layer-2 pseudo-wires and layer-1 connections;

[0059]   – decoupling signalling and routing;

[0060]   – allowing signalling to possibly traverse a network differently than the datapath;

[0061]   – allowing Martini-based encapsulation protocols to be used with other signalling protocols (other than LDP) including standard-based or proprietary layer-2-based signalling protocols;

[0062]   •   inherent interactivity with IP networking protocols:

[0063]   – with or without MPL datapath; and

[0064]   – including support for IP tunnelling including MPLS-in-IP encapsulation;

[0065]   •   support of encapsulation protocols, including:

[0066]   – existing standards; and

[0067]   – Martini-based encapsulation;

[0068]   •   signalling uses native transport signalling when a signalling choice is required.

[0069]   The generalized L2 VPN mechanisms are illustrated in **FIG. 2** where the GL2VPN **201** has two distinct operations: the Generalized Pseudo-Wire operations **202**, and the VPN Constructs operations **203**. Subsumed under the Generalized Pseudo-Wire operations **202** are the Encapsulation operations **204**, Generic Single-Sided Signalling operations **206** and Quality-of-Service/SLA operations **208**. Subsumed under the VPN Constructs operations **203** are the Generalized Auto-Discovery operations **205** and the Membership operations **207**. Martini-based encapsulation protocols **210** are specifically referenced under Encapsulation operations **204**.

[0070]   Referring to **FIG. 3** there may be seen a schematic diagram showing network-side services in relation to access-side services. On the Network-Side **301** may be seen services such as GMPLS/IP **303**, MPLS/IP **305**, ATM Networking **307**, Ethernet Networking **309**, Legacy DPRS **311**, and proprietary services such as PORS **313**. On the Access-Side **302** may be seen services such as SONET **304**, Frame Relay **306**, ATM **308**, and Ethernet **310**.

[0071]   Referring to **FIG. 4** there may be seen the same schematic diagram showing network-side services in relation to access-side services with a connection **420** established from the Access-Side **402** to the Network-Side **401**. The Generalized Pseudo-Wire function **440** served by the generalized Layer-2 VPN may be seen in schematic diagram as facilitating a scalable and flexible any access-service to any network.

[0072]   Referring to **FIG. 5** there may be seen a diagram of the main modules of a generalized L2VPN system. The modules include GL2VPN Manager module **501**, a VPN-Service Discovery module **503**, a VPN-Network Discovery module **505**, a Generalized Single-Sided Signalling module **507**, and a Multi-Service Tunnel Selector module **509**. These modules coordinate the decisions and service and network selections. Coordinating with the GL2VPN Manager module **501** are the Connection Admission Control (CAC) module **511** and the Encapsulation Selector module **513**. The

Encapsulation Selector module will have a number of sub-modules related to different encapsulation protocols, for example, Martini-based Encapsulation Protocol **531**, Layer2 Tunnelling Protocol Version 3 **533**, Point-to-Point Common Header Protocol **535**, or Point-to-Point Subnet Header Protocol **537**. The GL2VPN Manager module **501** will coordinate at **502** with the VPN-Service Discovery module **503** such items as Standards-based "Smart" CAC, and Quality-of-Service/SLA handling. The VPN-Service Discovery module **503** handles examining connected networks to discover and appropriately propagate addressing for the plurality of L1VPNs, L2VPNs, and L3VPNs at **515**. Also visible is the connection between the GL2VPN Manager module **501** and the GEP GPW Endpoints **525**.

[0073] Thus, the foregoing has described a generalized Layer-2 virtual private network (GL2VPN) with advantages including the capability to support any Layer-2 and/or layer-1 VPN service to any network type using scalable common Layer-2 connections, and virtual private networks and without restricting the service provider to a particular transport or technology used within the provider network.

[0074] While the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all modifications, variations and adaptations such as may be made to the particular embodiments of the invention described above without departing from the scope of the invention, which is defined in the claims.